

Finding involutions with small support

Alice C. Niemeyer and Tomasz Popiel

ABSTRACT. We show that the proportion of permutations g in S_n or A_n such that g has even order and $g^{|g|/2}$ is an involution with support of cardinality at most $\lceil n^\varepsilon \rceil$ is at least a constant multiple of ε . Using this result, we obtain the same conclusion for elements in a classical group of natural dimension n in odd characteristic that have even order and power up to an involution with (-1) -eigenspace of dimension at most $\lceil n^\varepsilon \rceil$ for a linear or unitary group, or $2\lceil n/2 \rceil^\varepsilon$ for a symplectic or orthogonal group.

1. Introduction

Involutions and their centralisers are important not only in the Classification of Finite Simple Groups, but also in many algorithms for computing with finite groups, as can be seen from the numerous applications of Bray's algorithm [5] for finding the centraliser of an involution. In practice, involutions (elements of order 2) can be obtained by raising an element g of even order to the power of $|g|/2$, and this is especially useful in groups where involutions are rare. For example, in a finite symmetric group S_n or alternating group A_n , algorithms that obtain involutions in this way include those in [2, 3, 4, 6]. The algorithms in [2, 3, 4] require transpositions, while the algorithm in [6] requires involutions with support of cardinality at most a constant times \sqrt{n} (the *support* of a permutation being the set of points that it moves). Although involutions in S_n or A_n are rare, it was proved in [6, Theorem 1.2] that the proportion of elements g in S_n or A_n that have even order and for which the support of $g^{|g|/2}$ has cardinality at most $4\sqrt{n}/3$ is at least $(13 \log(n))^{-1}$. Here we strengthen this result considerably.

THEOREM 1.1. *Let $\varepsilon \in (0, 1)$, and let n be an integer satisfying $\lceil (\log(n) + 1)^2 \rceil < \lceil n^\varepsilon \rceil \leq n - 2\lceil \log(n) \rceil$. Let $p(n, \varepsilon)$ denote the proportion of elements $g \in S_n$ such that g has even order and $g^{|g|/2}$ is an involution whose support has cardinality at most $\lceil n^\varepsilon \rceil$, and let $\tilde{p}(n, \varepsilon)$ denote the corresponding proportion of elements in A_n . Then $p(n, \varepsilon) > \varepsilon/48$ and $\tilde{p}(n, \varepsilon) > \varepsilon/96$.*

Involutions play an important role in several algorithms for computing with matrix groups or black-box groups; see, for example, the survey article by O'Brien [9]. As an application of Theorem 1.1, we obtain a lower bound for the proportion of elements in a classical group in odd characteristic that have even order and power up to an involution with a (-1) -eigenspace of 'small' dimension. Here, for a finite group H and a subset I of involutions in H , we write $P(H, I) = \{h \in H : |h| \text{ is even and } h^{|h|/2} \in I\}$.

THEOREM 1.2. *Let $\varepsilon \in (0, 1)$, and let ℓ be an integer satisfying $\lceil (\log(\ell) + 1)^2 \rceil < \lceil \ell^\varepsilon \rceil \leq \ell - 2\lceil \log(\ell) \rceil$. Let q be a power of an odd prime, and let $n = n(\ell)$, $S = S(n, q)$, $X = X(n, q)$, α and c_1 be as in one of the lines of Table 1. Let H be a group satisfying $S \leq H \leq X$, and define $c_2 = 1/4$ if $S < H \leq X$ in lines 3–5 of Table 1, and $c_2 = 1$ otherwise. Define I to be the set of involutions in H that have (-1) -eigenspace of dimension r such that $r \leq \alpha \lceil \ell^\varepsilon \rceil$. Then $|P(\overline{H}, \overline{I})|/|\overline{H}| \geq |P(H, I)|/|H| > c_1 c_2 \cdot \varepsilon/48$, where $\overline{H} = H/Z(H)$ and $\overline{I} = IZ(H)/Z(H)$, with $Z(H)$ the centre of H .*

Theorems 1.1 and 1.2 are proved in Sections 2 and 3, respectively.

2010 *Mathematics Subject Classification.* primary 20D06; secondary 20P05, 20B30.

Key words and phrases. symmetric group, alternating group, classical group, proportion of elements, involution.

This research forms part of the Australian Research Council Discovery Project DP140100416. The second author thanks RWTH Aachen University for financial support and hospitality during his visit in September 2015.

n	S	X	α	c_1
ℓ	$\mathrm{SL}_n(q)$	$\mathrm{GL}_n(q)$	1	$1/2$
ℓ	$\mathrm{SU}_n(q)$	$\mathrm{GU}_n(q)$	1	$1/2$
2ℓ	$\mathrm{Sp}_n(q)$	$\mathrm{GSp}_n(q)$	2	$1/4$
$2\ell + 1$	$\mathrm{SO}_n(q)$	$\mathrm{GSO}_n(q)$	2	$1/4$
2ℓ	$\mathrm{SO}_n^\pm(q)$	$\mathrm{GO}_n^\pm(q)^\circ$	2	$1/4$

TABLE 1. Definitions for Theorem 1.2.

2. Proof of Theorem 1.1

We first prove the result for S_n . Let a be a positive integer, and k an odd positive integer with $2^a k \leq n$. Consider a permutation $g \in S_n$ with a cycle of length $2^a k$, and the remaining $n - 2^a k$ points lying in cycles of lengths not divisible by 2^a . Then the permutation $g^{\lfloor g \rfloor/2}$ is an involution whose support has cardinality $2^a k$. In particular, consider those such permutations for which $a \leq A := \log_2(\lceil \log(n) \rceil)$ and $k \leq K := \lfloor \lceil n^\varepsilon \rceil / \lceil \log(n) \rceil \rfloor$, so that $2^a k \leq \lceil n^\varepsilon \rceil$. Noting that the proportion of $(2^a k)$ -cycles in S_n is $1/(2^a k)$, and letting $s_{-2^a}(\ell)$ denote the proportion of elements in S_ℓ (for some ℓ) with no cycles of lengths divisible by 2^a , we have

$$(1) \quad p(n, \varepsilon) \geq \sum_{\substack{k=1 \\ k \text{ odd}}}^K \sum_{a=1}^A \frac{s_{-2^a}(n - 2^a k)}{2^a k}.$$

Now, $n \geq \lceil n^\varepsilon \rceil + 2 \lceil \log(n) \rceil \geq (k+2) \lceil \log(n) \rceil \geq 2^a (k+2)$, so $2^a \leq (n - 2^a k)/2$. Hence, we may apply [7, Lemma 4.2(a)] (a consequence of [1, Theorem 2.3(b)]), which gives $s_{-2^a}(n - 2^a k) \geq (4(n - 2^a k))^{-1/(2^a)}$. Therefore,

$$\begin{aligned} p(n, \varepsilon) &\geq \frac{1}{4} \sum_{\substack{k=1 \\ k \text{ odd}}}^K \sum_{a=1}^A \frac{1}{2^a k (n - 2^a k)^{1/2^a}} \\ &> \frac{1}{4} \sum_{\substack{k=1 \\ k \text{ odd}}}^K \sum_{a=1}^A \frac{1}{2^a k n^{1/2^a}} = \frac{1}{4} \left(\sum_{\substack{k=1 \\ k \text{ odd}}}^K \frac{1}{k} \right) \left(\sum_{a=1}^A \frac{1}{2^a n^{1/2^a}} \right). \end{aligned}$$

Writing $2m + 1 = k$ and $K' = \lfloor (K - 1)/2 \rfloor$, we have

$$p(n, \varepsilon) > \frac{1}{4} \left(\sum_{m=0}^{K'} \frac{1}{2m+1} \right) \left(\sum_{a=1}^A \frac{1}{2^a n^{1/2^a}} \right).$$

Since $1/(2m+1)$ is decreasing in m and $(2^a n^{1/2^a})^{-1}$ is increasing in a , we can bound the above sums by integrals as follows:

$$\begin{aligned} (2) \quad p(n, \varepsilon) &> \frac{1}{4} \left(\int_0^{K/2} \frac{dx}{2x+1} \right) \left(\int_0^A \frac{dx}{2^x n^{1/2^x}} \right) \\ &= \frac{1}{4} \left[\frac{\log(2x+1)}{2} \right]_0^{K/2} \left[\frac{1}{\log(2) \log(n) n^{1/2^x}} \right]_0^A \\ &= \frac{\log(K+1)}{8 \log(2) \log(n)} \left(\frac{1}{n^{1/2^A}} - \frac{1}{n} \right). \end{aligned}$$

Since $K = \lfloor \lceil n^\varepsilon \rceil / \lceil \log(n) \rceil \rfloor > \lceil n^\varepsilon \rceil / \lceil \log(n) \rceil - 1 \geq n^\varepsilon / (\log(n) + 1) - 1$, we have $K+1 > n^\varepsilon / (\log(n) + 1)$. Therefore,

$$p(n, \varepsilon) > \frac{1}{8 \log(2)} \left(\varepsilon - \frac{\log(\log(n) + 1)}{\log(n)} \right) \left(\frac{1}{e} - \frac{1}{n} \right).$$

Since $\lceil n^\varepsilon \rceil > \lceil (\log(n) + 1)^2 \rceil$, we have $n^{\varepsilon/2} > \log(n) + 1$, and so the term in the first set of parentheses above is at least $\varepsilon/2$. Hence,

$$(3) \quad p(n, \varepsilon) > \frac{\varepsilon}{16 \log(2)} \left(\frac{1}{e} - \frac{1}{n} \right).$$

Since $n \geq \lceil n^\varepsilon \rceil + 2\lceil \log(n) \rceil > \lceil (\log(n) + 1)^2 \rceil + 2\lceil \log(n) \rceil$, we have, in particular, $n \geq 27$. Therefore, $1/e - 1/n > \log(2)/3$, and hence $p(n, \varepsilon) > \varepsilon/48$.

The proof for A_n requires only minor changes. We again consider permutations with a cycle of length $2^a k$ and the remaining $n - 2^a k$ points lying in cycles of length not divisible by 2^a , but now the product of the cycles not divisible by 2^a should lie in $S_n \setminus A_n$. Let $\mathbf{a}_{-2^a}(\ell)$ and $\mathbf{c}_{-2^a}(\ell)$ denote, respectively, the proportions of elements in A_ℓ and $S_\ell \setminus A_\ell$ (for some ℓ) with no cycles of lengths divisible by 2^a . Since $\mathbf{c}_{-2^a}(\ell) = 2\mathbf{s}_{-2^a}(\ell) - \mathbf{a}_{-2^a}(\ell)$, [1, Theorem 3.3(b)] gives $\mathbf{c}_{-2^a}(\ell) \geq (1 - 1/(2^a - 1))\mathbf{s}_{-2^a}(\ell)$. For $a \geq 2$, we therefore have $\mathbf{c}_{-2^a}(\ell) \geq 2/3 \cdot \mathbf{s}_{-2^a}(\ell)$, and so the inequality (1) is replaced by

$$\tilde{p}(n, \varepsilon) \geq \frac{2}{3} \sum_{\substack{k=1 \\ k \text{ odd}}}^K \sum_{a=2}^A \frac{\mathbf{s}_{-2^a}(n - 2^a k)}{2^a k}.$$

The range of the second integral in (2) is accordingly changed to $[1, A]$, and so instead of (3) we obtain

$$\tilde{p}(n, \varepsilon) > \frac{2}{3} \cdot \frac{\varepsilon}{16 \log(2)} \left(\frac{1}{e} - \frac{1}{\sqrt{n}} \right).$$

Since $n \geq 27$, we have $1/e - 1/\sqrt{n} > \log(2)/4$, and hence $\tilde{p}(n, \varepsilon) > \varepsilon/96$.

REMARK 2.1. If the single cycle of length $2^a k$ in the proof of Theorem 1.1 is replaced by a product of cycles of lengths divisible by 2^a but not by 2^{a+1} , then the resulting permutation g still powers up to an involution with support at most $\lceil n^\varepsilon \rceil$. By [6, Lemma 5.2] (a refinement of a particular case of [8, Theorem 1.1]), the proportion $t_{2^a}(2^a k)$ of elements in $S_{2^a k}$ with all cycles of lengths divisible by 2^a but not by 2^{a+1} is at least $c(a)/k^{1-1/2^{a+1}}$, where $c(a) = 1/(2^{2a} 3^{1/2^{a+1}})$. For a fixed value of a , this lower bound, viewed as a function of k , is asymptotically better than the lower bound of $1/(2^a k)$ that we have employed in the proof of Theorem 1.1, and it was used in the proof of [6, Theorem 1.2], where only two values of a were considered. However, in the proof of Theorem 1.1, where we sum over a range of values of a that depends on n , the lower bound $c(a)/k^{1-1/2^{a+1}}$ for $t_{2^a}(2^a k)$ is too small to yield a constant lower bound for $p(n, \varepsilon)$, and so we have opted to use the ‘weaker’ bound $1/(2^a k)$.

3. Proof of Theorem 1.2

The proof is essentially the same as that of [7, Theorem 1.1], but we change the range of r from $r \in [n/3, 2n/3]$ to $r \leq \alpha \lceil \ell^\varepsilon \rceil$. Consider first the case where $H = \mathrm{GL}_n(q)$ or $\mathrm{GU}_n(q)$, and let W be the Weyl group of H , noting that $W \cong S_n$. We modify the definition of $M(a) \subset W$ from [7, Section 5(ii)] as follows: an element $w \in W$ lies in $M(a)$ if and only if it contains a cycle of length $2^a k$ for some odd integer k with $2^a k \leq \lceil \ell^\varepsilon \rceil = \lceil n^\varepsilon \rceil$, and no other cycle has length divisible by 2^a . The argument in [7, Section 5(ii)] is then still valid, and hence we still obtain [7, Equation (5)], which gives $|P(H, I)|/|H| \geq p(n, \varepsilon)/2$, showing that $c_1 = 1/2$. If $H = \mathrm{Sp}_{2\ell}(q)$, $\mathrm{SO}_{2\ell+1}(q)$ or $\mathrm{SO}_{2\ell}^\pm(q)$, then the argument in [7, Section (vii)] still applies: the Weyl group is now a subgroup of $S_2 \wr S_\ell$, $M(a)$ is redefined so that the cycle of length $2^a k \leq \lceil \ell^\varepsilon \rceil$ is positive, and we conclude that $c_1 = 1/4$. The same arguments as in [7, Sections (v) and (viii)] give the claimed values for c_2 . Finally, the proof of [7, Corollary 1.2] gives the result for the groups \overline{H} .

References

- [1] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger, and Á. Seress, ‘Permutations with restricted cycle structure and an algorithmic application’, *Combin. Probab. Comput.* **11** (2002), 447–464.
- [2] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger, and Á. Seress, ‘A black-box group algorithm for recognizing finite symmetric and alternating groups. I’, *Trans. Amer. Math. Soc.* **355** (2003), 2097–2113.
- [3] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger, and Á. Seress, ‘Constructive recognition of finite alternating and symmetric groups acting as matrix groups on their natural permutation modules’, *J. Algebra* **292** (2005), 4–46.

- [4] S. Bratus and I. Pak, ‘Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach’s conjecture’, *J. Symbolic Comput.* **29** (2000), 33–57.
- [5] J. N. Bray, ‘An improved method for generating the centralizer of an involution’, *Arch. Math. (Basel)* **74** (2000), 241–245.
- [6] S. Jambor, M. Leuner, A. C. Niemeyer, and W. Plesken, ‘Fast recognition of alternating groups of unknown degree’, *J. Algebra* **392** (2013), 315–335.
- [7] F. Lübeck, A. C. Niemeyer, and C. E. Praeger, ‘Finding involutions in finite Lie type groups of odd characteristic’, *J. Algebra* **321** (2009), 3397–3417.
- [8] A. C. Niemeyer, T. Popiel, C. E. Praeger, and Ş. Yalçınkaya, ‘On semiregular permutations of a finite set’, *Math. Comp.* **81** (2012), 605–622.
- [9] E. A. O’Brien, ‘Algorithms for matrix groups’, in: *Groups St. Andrews 2009 in Bath, II*, London Mathematical Society Lecture Note Series, 388 (Cambridge University Press, Cambridge, 2011), pp. 297–323.

LEHR- UND FORSCHUNGSGEBIET ALGEBRA, RWTH AACHEN UNIVERSITY, 52062 AACHEN, GERMANY.
EMAIL: ALICE.NIEMEYER@MATH.RWTH-AACHEN.DE.

CENTRE FOR THE MATHEMATICS OF SYMMETRY AND COMPUTATION, SCHOOL OF MATHEMATICS AND STATISTICS,
THE UNIVERSITY OF WESTERN AUSTRALIA, 35 STIRLING HIGHWAY, CRAWLEY, W.A. 6009, AUSTRALIA.
EMAIL: TOMASZ.POPIEL@UWA.EDU.AU.